

LAMPS
Internet-Draft
Updates: [5480](#) (if approved)
Intended status: Standards Track
Expires: September 30, 2020

T. Ito
SECOM CO., LTD.
S. Turner
sn3rd
March 31, 2020

Clarifications for Elliptic Curve Cryptography Subject Public Key
Information
draft-ietf-lamps-5480-ku-clarifications-03

Abstract

This document updates [RFC 5480](#) to specify semantics for the keyEncipherment and dataEncipherment key usage bits when used in certificates that support Elliptic Curve Cryptography.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 30, 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

[1.](#) Introduction [2](#)

[2.](#) Terminology [2](#)

[3.](#) Updates to [Section 3](#) [2](#)

[4.](#) Security Considerations [3](#)

[5.](#) IANA Considerations [3](#)

[6.](#) Normative References [3](#)

Authors' Addresses [3](#)

[1.](#) Introduction

[RFC5480] specifies the syntax and semantics for the Subject Public Key Information field in certificates that support Elliptic Curve Cryptography. As part of these semantics, it defines what combinations are permissible for the values of the key usage extension [RFC5280]. [RFC5480] specifies 7 of the 9 values; it makes no mention of keyEncipherment and dataEncipherment key usage bits. This document corrects this omission, by updating [Section 3 of \[RFC5480\]](#) to make it clear that neither keyEncipherment nor the dataEncipherment key usage bits are set for key agreement algorithms defined therein. The additions are to be made to the end of [Section 3](#).

[2.](#) Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14 \[RFC2119\]](#) [RFC8174] when, and only when, they appear in all capitals, as shown here.

[3.](#) Updates to [Section 3](#)

If the keyUsage extension is present in a certificate that indicates id-ecPublicKey in SubjectPublicKeyInfo, then following values MUST NOT be present:

- keyEncipherment; and
- dataEncipherment.

If the keyUsage extension is present in a certificate that indicates id-ecDH or id-ecMQV in SubjectPublicKeyInfo, then the following

values also MUST NOT be present:

keyEncipherment; and
dataEncipherment.

Ito & Turner

Expires September 30, 2020

[Page 2]

Internet-Draft

Clarifications for ECC SPKI

March 2020

4. Security Considerations

This document introduces no new security considerations beyond those found in [[RFC5480](#)].

5. IANA Considerations

This document makes no request of IANA.

6. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC 5280](#), DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", [RFC 5480](#), DOI 10.17487/RFC5480, March 2009, <<https://www.rfc-editor.org/info/rfc5480>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

Authors' Addresses

Tadahiko Ito

SECOM CO., LTD.

Email: tadahiko.ito.public@gmail.com

Sean Turner
sn3rd

Email: sean@sn3rd.com

Ito & Turner

Expires September 30, 2020

[Page 3]